

Fortify Scan Issue: Default rulepacks were not used during scan

VA Top 10 Fortify Scan Issues For 2016 (Q4)



This page has been made public for vendors

Question

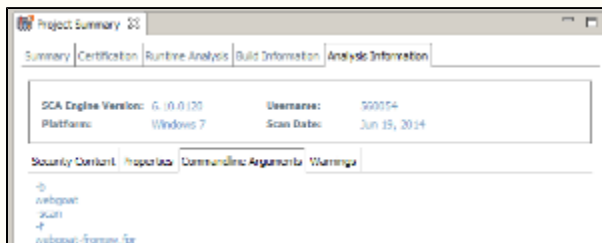
What does the Fortify scan issue "Default rulepacks were not used during scan" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that the full set of rulepacks provided by Fortify were not applied to the scan. While it is possible to select just the rulepacks that apply to the languages included in the application, using the full set of rulepacks avoids accidentally missing a rulepack that should be used. If a rulepack is not used that applies to an application, then the issues reported may be incomplete.

How to detect

Limiting the rulepacks used may be done on the command line, via Fortify properties, or through the options dialog in the IDEs. In each case, however, it is most likely to show up in the command line (setting the options to limit the rulepacks in any of the GUI interfaces results in changing the command line). To look at the command line, open up the Project Summary in Audit Workbench or your IDE, select the Analysis Information tab and the Commandline Arguments sub-tab:



On the command line, look for any of the following options that indicate that either the rulepacks being used are limited or rules from the rulepacks are being limited:

- -no-default-rules
- -rules
- -no-default-issue-rules
- -no-default-source-rules
- -no-default-sink-rules

Properties may be viewed in the properties sub-tab in the Project Summary. There are corresponding properties to each of the command line options.

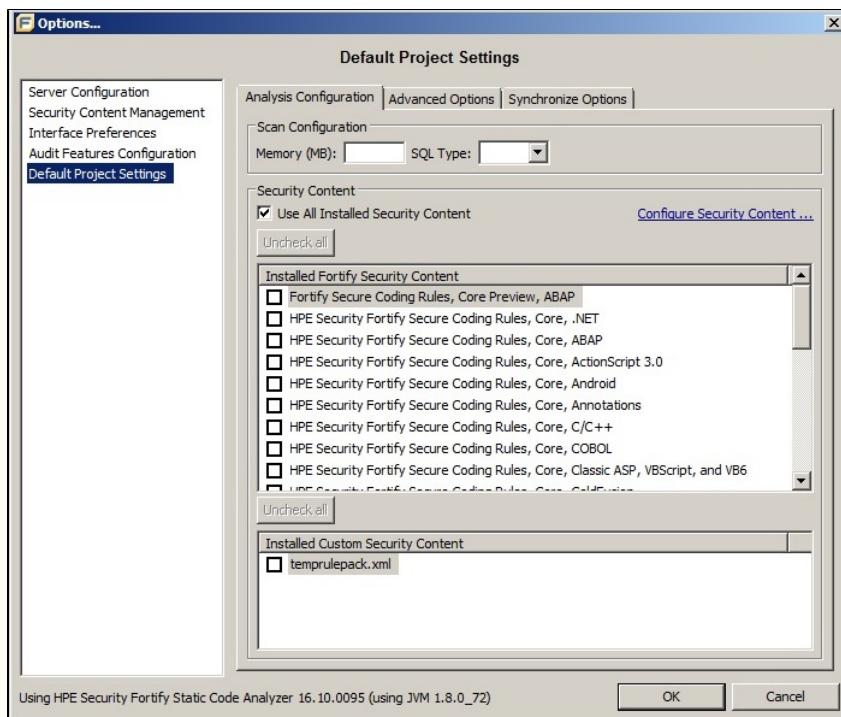
How to resolve

Fortify's default is to use all the rulepacks. To limit the rulepacks used, they must be explicitly limited in either the Audit Workbench or IDE options dialog or explicitly limited in the command line or properties configuration. Resolve this issue by removing any explicit limitation to which rulepacks are to be used for the scan and rescan the application.

If they were limited in the IDEs, for example, open the HP Fortify -> Options dialog, select Default Project Settings and the Analysis Configuration tab. Select the "Use All Installed Security Content" check box to ensure all the rulepacks are used as illustrated below:

HPE Fortify Version	4.30 and later
Programming Language	<input checked="" type="checkbox"/> C/C++ <input checked="" type="checkbox"/> .NET <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Objective-C <input checked="" type="checkbox"/> Other
Fortify Audit Workbench	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Fortify IDE Plugin	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Other Fortify Component	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Request code review tools, validations, and support [HERE](#).



References

- [VA Top 10 Fortify Scan Issues For 2016 \(Q4\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q3\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q2\)](#)
- [VA Top 10 Fortify Scan Issues For 2015 \(Q1\)](#)